IC card

Patent Number: US4885788

Publication date: 1989-12-05

Inventor(s): TAKARAGI KAZUO (JP); SHIRAISHI TAKAYOSHI (JP); SASAKI RYOICHI (JP) (JP)

Applicant(s): HITACHI LTD (JP)

Requested Patent: DE3704814

Application Number: US19870013800 19870212

Priority Number(s): JP19860030815 19860217

IPC Classification: H04L9/00

EC Classification: G06K19/073, G07F7/10D10M

Equivalents: JP2036313C, JP62189593, JP7054536B

Abstract

An IC card having an authentication code which is compared with an authentication code obtained by processing data recorded on the IC card, and permitting the IC card to be used only when agreement is found.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Patentschrift**

(10) **DE 37 04 814 C 3**

(51) Int. Cl.[7]: **G 06 K 19/073**

(21) Aktenzeichen: P 37 04 814.7-53
(22) Anmeldetag: 16. 2. 1987
(43) Offenlegungstag: 20. 8. 1987
(45) Veröffentlichungstag der Patenterteilung: 2. 5. 1996
(45) Veröffentlichungstag des geänderten Patents: 28. 12. 2000

Patentschrift nach Einspruchsverfahren geändert

(30) Unionspriorität:
P 30815/86 17. 02. 1986 JP

(73) Patentinhaber:
Hitachi, Ltd., Tokio/Tokyo, JP

(74) Vertreter:
Strehl, Schübel-Hopf & Partner, 80538 München

(72) Erfinder:
Takaragi, Kazuo, Yokohama, Kanagawa, JP;
Shiraishi, Takayoshi, Chigasaki, Kanagawa, JP;
Sasaki, Ryoichi, Fujisawa, Kanagawa, JP

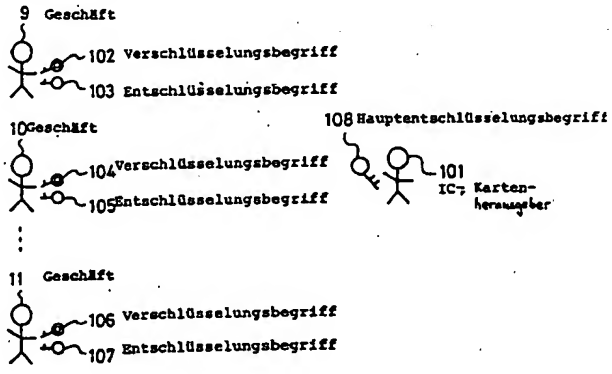
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 29 17 965 A1
EP 01 52 024 A2

MEYER, Carl H., MATYAS, M.: Cryptography: A New Dimension In Computer Data Security, John Wiley & Sons, New York 1982, S. 517-520, 551-557;
GLASS, S., MASSEY, J.L: Plastikkarten - wie intelligent ist sicher? "Landis & Gyr Mitteilungen 32 (1985), S. 22-32;

(54) Karte mit integrierter Schaltung

(57) IC-Karte zum bidirektionalen Datentransfer mit einer Vielzahl von Terminals (9 bis 11), auf der ein Berechtigungscode für die Benutzung der Vielzahl von Terminals durch einen Benutzer (16) der IC-Karte gespeichert und auf der ein Speicher (19) vorgesehen ist, der in eine Vielzahl von Bereichen (22 bis 24) aufgeteilt ist, dadurch gekennzeichnet, daß
jedem der Bereiche ein eigenes Verschlüsselungs- und Entschlüsselungsbegriffspaar (102 bis 107) zugeordnet ist,
wobei die verschiedenen Verschlüsselungs- und Entschlüsselungsbegriffspaare jeweils einer Anzahl von Personen, die die Terminals (9 bis 11) betreiben, bekanntgegeben werden, um die IC-Karte für diese Anzahl von Personen verwendbar zu gestalten,
wobei die Daten jedes Bereiches bei Eingabe des dem Bereich zugeordneten Verschlüsselungsbegriffes an einem der Terminals verschlüsselt werden, und
wobei die Daten jedes Bereiches bei Eingabe des dem Bereich zugeordneten Entschlüsselungsbegriffes an einem der Terminals entschlüsselt werden.



DE 37 04 814 C3

DE 37 04 814 C3

Beschreibung

Die Erfindung betrifft eine IC-Karte gemäß dem Oberbegriff des Patentanspruchs. Eine solche IC-Karte zum bidirektionalen Datentransfer mit Terminals ist aus der EP 0 152 024 A2 bekannt. Eine IC-Karte, auf der ein Berechtigungscode für die Benutzung der Terminals durch eine Person gespeichert ist, ist auch aus der DE 29 17 965 A1 bekannt.

Eine IC-Karte, die aus eine Kunststoffkartenkörper, in den ein IC, d. h. eine integrierte Schaltung eingebettet ist, soll eine einzelne Person identifizieren, eine Fälschung erschweren und eine große Speicherkapazität haben und findet ihre Anwendung bei der elektronischen Abrechnung, bei Personalinformationskarteien, der Sicherheitskontrolle u. ä.

Wenn eine Person in Supermärkten oder Warenhäusern unter Verwendung einer einzelnen IC-Karte einkauft, ist es vom Standpunkt der Beibehaltung der Vertraulichkeit wünschenswert, daß eine Liste von Käufen in einem Geschäft nicht in anderen Geschäften gelesen werden kann, in denen der Kunde andere Käufe tätigt. Zu diesem Zweck sollte die IC-Karte mit Transaktionsbereichen versehen sein, die in Abhängigkeit von den Geschäften verschieden sind, so daß ein Geschäft keinen Bezug auf die Transaktionen von anderen Geschäften nehmen kann.

Bisher besteht eine erste Schwierigkeit darin, daß es weder ein Verfahren zum Schützen einer Vielzahl von Transaktionsbereichen in derselben IC-Karte über verschiedene Verschlüsselungsbegriffe noch ein dazu geeignetes Schlüsselsteuerverfahren gibt. Unter den öffentlichen Verschlüsselungssystemen gibt es andererseits beim RAS-Verfahren und beim Rabin-Verfahren einen Hauptschlüssel. Unter Verwendung des Hauptschlüssels kann die oben erwähnte Schlüsselsteuerung wirksam ausgeführt werden.

Eine zweite Schwierigkeit besteht bisher darin, daß die Fälschung der IC-Karte und die Änderung oder Fälschung von Daten in der Karte nicht berücksichtigt wurden.

Eine dritte Schwierigkeit besteht darin, daß die herkömmliche IC-Karte unter der Voraussetzung hergestellt wurde, daß sie von einer einzelnen Person benutzt wird (siehe Nikkei Computer "Will the Age of IC Card will Come?", 8. Juli 1985). Gesundheitsdaten, Vermögensdaten und ähnliche Daten können der IC-Karte eingegeben werden, um diese zu benutzen. Zusätzlich zu dem Fall, in dem der Benutzer selbst die Personenidentifizierungsnummer eingibt, um die gewünschten Daten zu erhalten, kommt es jedoch auch oft vor, daß ein Arzt oder ein Bankangestellter eine andere Personenidentifizierungsnummer eingibt, um alle gewünschten Daten oder einen Teil der gewünschten Daten, beispielsweise in einem Notfall, zu entnehmen.

Aufgabe der Erfindung ist es, die bekannte IC-Karte so aus zubilden, daß sie für eine Anzahl von Personen verwendbar ist, aber jede Person nur auf bestimmte Bereiche des Speichers der IC-Karte Zugriff hat.

Diese Aufgabe wird bei einer gattungsgemäßen IC-Karte durch die im kennzeichnenden Teil des Patentanspruchs angegebenen Maßnahmen gelöst.

Die erfindungsgemäße IC-Karte soll es insbesondere möglich machen, eine Fälschung der. Karte oder eine Fälschung oder Änderung der Daten in der Karte, beispielsweise einer bargeldlosen Einkaufskreditkarte festzustellen.

Die erfindungsgemäße IC-Karte soll es schließlich dem Benutzer der Karte erlauben, die Daten zu entnehmen und gleichfalls nur einem begrenzten Personenkreis möglich machen im Notfall Daten zu entnehmen.

Dazu wird gemäß der Erfindung beim Einschreiben der Daten an den Transaktionsbereichen der IC-Karte oder beim Lesen der Daten von diesen Transaktionsbereichen der folgende Arbeitsablauf ausgeführt.

(i) Der IC-Karten-Herausgeber oder -Verwalter bereitet vorher Gruppen von Verschlüsselungs- und Entschlüsselungsbegriffen in der Anzahl der Transaktionsbereiche vor, die geheimgehalten werden, und bildet einen Hauptentschlüsselungsbegriff für alle Entschlüsselungsbegriffe.

(ii) Der Kartenverwalter- oder -herausgeber ordnet einen Verschlüsselungsbegriff und einen Entschlüsselungsbegriff jedem Transaktionsbereich zu, schreibt einen oberen verfügbaren Geldbetrag und den Verschlüsselungsbegriff oder den Entschlüsselungsbegriff an einem Teil des Transaktionsbereiches ein und verschlüsselt den obigen Transaktionsbereich unter Verwendung des Verschlüsselungsbegriffes.

(iii) Der IC-Kartenverwalter oder -herausgeber übergibt die IC-Karte dem Benutzer. Er händigt weiterhin den Verschlüsselungsbegriff und den Entschlüsselungsbegriff den einzelnen Geschäften aus, so daß diese die Transaktionsbereiche ver- und entschlüsseln können.

Aufgrund der oben beschriebenen Arbeitsvorgänge (i) bis (iii) haben die verschiedenen Geschäfte verschiedene Verschlüsselungs- und Entschlüsselungsbegriffe. Ein gegebenes Geschäft kann daher nur die Transaktionsbereiche, die dem Entschlüsselungs- und Verschlüsselungsbegriff entsprechen, die das Geschäft hat, aus einer Vielzahl von Transaktionsbereichen verarbeiten, die in der IC-Karte enthalten sind. Das macht es möglich, die Vertraulichkeit für den Benutzer zu schützen. Der IC-Karten-Herausgeber hält den Hauptentschlüsselungsbegriff, der willkürlich alle Transaktionsbereiche der IC-Karte entschlüsseln kann, um deren Inhalt kennenzulernen. Der Hauptentschlüsselungsbegriff kann daher dann benutzt werden, wenn die einzelnen Entschlüsselungsbegriffe verlorengegangen sind. Der Hauptentschlüsselungsbegriff muß weiterhin nicht für die Transaktionen verwandt werden, er kann sicher aufbewahrt werden.

Gemäß der Erfindung werden weiterhin die Daten in der Karte dadurch erfaßt, daß der Saldo und eine Datenänderungscodierung geprüft werden, um mit Änderungen der Daten fertigzuwerden. Die Datenänderung in der Geschäftstransaktionsdatei oder in der Banktransaktionsdatei wird weiterhin dadurch geprüft, daß die Datenänderungscodierung und die IC-Kartendaten gemischt und sortiert werden.

Eine Datenänderungsdetektorschaltung ähnelt im Prinzip dem Algorithmus einer Codefehlerdetektorschaltung und kann dadurch verwirklicht werden, daß eine Verschlüsselungsvorrichtung verwandt wird und deren Ausgangsdaten zum Eingang rückgekoppelt werden.

Schließlich kann ein Mikroprozessor der IC-Karte auf der Grundlage der eingegebenen Personenidentifizierungsnummer (zusätzlich zu Nummern sind auch Codierungen akzeptabel) die Zulässigkeitsstufe festlegen, und kann ein zugreifbarer Datenbereich bestimmt werden, um die erlaubten Daten zu liefern.

Im folgenden werden anhand der zugehörigen Zeichnung besonders bevorzugte Ausführungsbeispiele der Erfindung näher beschrieben. Es zeigen

Fig. 1A und 1B in Blockschaltbildern den Aufbau eines ersten Ausführungsbeispiels der erfindungsgemäßen IC-Karte,

Fig. 2 das Flußdiagramm eines Arbeitsablaufes, wenn der Benutzer einen Kauf in einem Geschäft unter Verwendung der IC-Karte tätigt,

Fig. 3 in einem Blockschaltbild den Aufbau eines zweiten

Ausführungsbeispiels der erfindungsgemäßen IC-Karte während des Einkaufs,

Fig. 4 in einem Blockschaltbild den Aufbau der Datenänderungsdetektorschaltung in der IC-Karte,

Fig. 5 in einem Blockschaltbild den Aufbau eines dritten Ausführungsbeispiels der erfindungsgemäßen IC-Karte bei einem IC-Kartensystem für Gesundheitsdaten,

Fig. 6 in einem Diagramm den Datenaufbau in einem Festspeicher ROM und

Fig. 7 in einem Diagramm den Datenaufbau in einem EEROM.

Die Fig. 1A und 1B zeigen den Aufbau eines ersten Ausführungsbeispiels der erfindungsgemäßen IC-Karte.

Eine derartige IC-Karte wird zunächst in der folgenden Weise vorbereitet.

Ein IC-Kartenherausgeber **101** bereitet Gruppen **102, 103, 106, 107** von Verschlüsselungsbegriffen und Entschlüsselungsbegriffen sowie einen Hauptentschlüsselungsbegriff **108** für die Entschlüsselungsbegriffe **103** . . . **107** vor und hält den Hauptentschlüsselungsbegriff geheim. Danach übergibt der IC-Kartenherausgeber **101** die Gruppen **102, 103** . . . **106, 107** von Verschlüsselungs- und Entschlüsselungsbegriffen den Geschäften **9** . . . **11**. Der IC-Kartenherausgeber schreibt weiterhin einen verfügbaren oberen Geldbetrag in die Transaktionsbereiche **22** . . . **24**. Der IC-Kartenherausgeber verschlüsselt dann die Gruppen **102, 103, 106, 107** der Verschlüsselungs- und Entschlüsselungsbegriffe mit dem Verschlüsselungsbegriff, der jeder der Karten entspricht, und schreibt jeweils eine Schlüsselbegriffsgruppe in jeden Schlüsselspeicher **13** . . . **15** der IC-Karte **25**. Dann verschlüsselt er die Berechtigungscodierungen entsprechend den an jedem Transaktionsbereich eingeschriebenen Daten mit dem Verschlüsselungsbegriff, der jeder der Karten entspricht, und schreibt diese Codierungen nieder. Der IC-Karten-Herausgeber übergibt dann die IC-Karte **25** einem Benutzer **16**.

Die Berechtigungscodierung bezieht sich dabei auf die Daten, die an den Transaktionsbereichen eingeschrieben sind, die komprimiert sind.

Über einen Eingabe/Ausgabeteil **12** werden Daten in einen Speicher **19** eingeschrieben und vom Speicher **19** gelesen, indem ein Prozessor **17** unter der Steuerung einer Software oder eines Programmpaketes betrieben wird, das in einem Festspeicher **18** enthalten ist.

Fig. 2 zeigt ein Flußdiagramm für den Arbeitsablauf der IC-Karte, wenn der Benutzer **16** einen Kauf in einem Geschäft **9** tätigt.

201 Der Benutzer gibt seine Personenidentifikationsnummer über den Eingabe/Ausgabeteil in den Prozessor **17** ein.
202 Der Prozessor **17** entnimmt die Personenidentifikationsnummer von einem geheimen Bereich unter der Steuerung der Software.
203 Der Prozessor **17** erzeugt über den Eingabe/Ausgabeteil ein zustimmendes Signal "in Ordnung", wenn die Personenidentifizierungsnummer, die vom Benutzer **16** eingegeben wurde, mit der Personenidentifizierungsnummer übereinstimmt, die im geheimen Bereich enthalten ist, erzeugt ein negatives Signal "nein", wenn das nicht der Fall ist.
204 Wenn das negative Signal erzeugt wird schreibt der Prozessor **17** keine Daten oder liest der Prozessor **17** keine Daten mehr, bis das positive Signal das nächstemal erzeugt wird.
205 Wenn das positive Signal erzeugt wird, erneuert das Geschäft **9** den Inhalt des Transaktionsbereiches **22** unter Verwendung des Verschlüsselungsbegriffes **102** und des Entschlüsselungsbegriffes **103** in Abhängigkeit von dem was der Benutzer **16** gekauft hat.

Im folgenden wird im einzelnen beschrieben, wie der Inhalt des Transaktionsbereiches neu geschrieben wird. Der Entschlüsselungsbegriff **103** wird nämlich in die IC-Karte **25** durch das Geschäft **9** eingegeben und die Daten im Schlüsselspeicher **13** werden mit dem Entschlüsselungsbegriff **103** entschlüsselt. Dann wird bestätigt, ob die Berechtigungscodierung, die in den entschlüsselten Daten enthalten ist, mit einer Berechtigungscodierung in Übereinstimmung steht, die aus den Daten des Transaktionsbereiches **22** berechnet wird. Nachdem diese Übereinstimmung bestätigt worden ist, werden der Transaktionsbereich **22** und die Berechtigungscodierung in Abhängigkeit von dem Wert des Kaufes neu geschrieben, woraufhin die Daten im Schlüsselspeicher **13** mit dem obigen Verschlüsselungsbegriff verschlüsselt werden.

Wenn sich jedoch herausstellt, daß die Berechtigungscodierungen nicht miteinander übereinstimmen, erzeugt die IC-Karte ein Signal, um das Geschäft **9** über diese Tatsache zu informieren, so daß das Geschäft **9** die notwendigen Maßnahmen ergreifen kann, um den Kauf zu unterbinden.

Im folgenden wird ein Beispiel eines Einkaufs unter Verwendung eines zweiten Ausführungsbeispiels der erfindungsgemäßen IC-Karte beschrieben.

Bei diesem Beispiel eines Einkaufs könnte ein unlauteres Geschäft dadurch zustandekommen, daß die Daten in der Karte geändert werden, beispielsweise die Daten des Bargeldempfangs von einer Bank und die Daten über den Verkauf und den Kauf geändert werden.

Fig. 3 zeigt das Blockschaltbild einer IC-Karte, die diese Art eines unlauteren Geschäftes verhindert.

Die IC-Karte kann nicht auf den nächsten Arbeitsvorgang übergehen, es sei denn, daß der Benutzer der IC-Karte durch eine Mischschaltung auf der Grundlage eines Kennwortes oder ähnlichem bestätigt wird. Eine Sicherheitscodierung **2** ist in einen Festspeicher eingeschrieben, der nicht direkt von außen gelesen werden kann. Eine Kontonummer **3** ist gleichfalls in den Festspeicher eingeschrieben. Eine Datenänderungsdetektorschaltung **4** bildet eine verschlüsselte Berechtigungscodierung, indem sie das Ausgangssignal einer Verschlüsselungsvorrichtung zu deren Eingangsseite rückkoppelt, wie es in Fig. 4 dargestellt ist. Wenn somit die Daten **61** . . . **64**, die zu autorisieren sind, geändert und als Daten **6** in Fig. 4 eingegeben werden, pflanzen sich die Auswirkungen der Bits der geänderten Daten der Reihe nach nach vorne fort und wird eine Codierung **65** gebildet, die sich von der ursprünglichen Codierung unterscheidet. Die Tatsache einer Datenänderung wird daher festgestellt.

Eine Eingabe/Ausgabesteuerschaltung **5** ist eine Schnittstellenschaltung zwischen der IC-Karte und den Terminals **30, 31** für die Karte. Eine Datei **6** betrifft die Eingabezeiten, die Terminal-Nummern, den Bargeldempfang und die Zahlungen, den Kontostand, die Datenänderungsfeststellungscodierung u. ä.

Um den Bargeldempfang auf die Karte zu schreiben, wird die Karte zunächst in ein Bankterminal **30** eingeführt und wird von der Tastatur aus ein Kennwort eingegeben. Das Kennwort wird über die Eingabesteuerschaltung **5** eingegeben und mit der Codierung in der Schaltung durch die Mischschaltung gemischt, um sicherzustellen, daß es sich bei der eingebenden Person um eine Person handelt, die Besitzer der Karte ist. Wenn das Mischergebnis positiv ist, wird die Konto-Nummer der Eingabe/Ausgabesteuerschaltung **5** auf ein Signal von der Mischschaltung **1** ansprechend zugeführt. Eine Konto-Datei wird dann am Bankterminal geöffnet. Wenn Bargeldempfangsdaten von der Tastatur der Karte eingegeben werden, wird eine Sicherheitscodierung am Terminal zusammen mit dem Bargeldempfang, der Zeit- dem

Kontostand und der Terminalnummer eingegeben. In der Karte werden die Daten, die durch die Eingabesteuerschaltung hindurchgegangen sind, der Datenänderungsfeststellungsschaltung **4** zugeführt, die eine Datenänderungsfeststellungscodierung dadurch bildet, daß sie die Zeit, die Terminalnummer und den Bargeldempfang als Eingangswerte der Verschlüsselungsvorrichtung mit der Sicherheitscodierung der Karte und der Sicherheitscodierung des Terminals als Kennbegriffe liefert. Diese Daten werden in die Datei **6** geschrieben und gleichzeitig in die Konto-Datei geschrieben. Die Sicherheitscodierung **2** des Terminals wird am Sicherheitscodierungsbereich der Karte aufgezeichnet. Der Sicherheitscodierungsbereich ist dabei ein Speicherbereich, der mit einer Einrichtung zum Schützen der Daten in Form einer Hardware und einer Software versehen ist, so daß die Daten durch eine außenstehende Person nicht entnommen werden können und keine Daten von einer außenstehenden Person eingeschrieben werden können.

Um in einem Geschäft einzukaufen, wird die Karte mit einem Einkaufsterminal **31** verbunden und wird ein Kennwort durch die Tastatur am Einkaufsterminal **31** eingegeben. Wenn das richtige Kennwort eingegeben wird, liest das Einkaufsterminal den Kontostand von der Karte. Nachdem der Kontostand geprüft ist, werden die Preise für die gekauften Waren über die Tastatur am Terminal **31** eingegeben. Wenn die Bargeldzahlung, die Zeit, der Kontostand, die Einkaufsterminalnummer und die Sicherheitscodierung am Terminal eingegeben werden, wie es oben beschrieben wurde, empfängt die Datenänderungsfeststellungsschaltung **4** in der Karte die Zeit **61**, die Terminalnummer **62**, den Bargeldempfang und die Zahlung **63** und den Kontostand **64** als Eingangsdaten, um eine Datenänderungsfeststellungscodierung **65** zusammen mit den Sicherheitscodierungen der Karte und des Terminals als Schlüsselbegriffe zu bilden. Diese Daten werden in die Datei **6** geschrieben und gleichzeitig über das Einkaufsterminal **31** zusammen mit der im Kontonummernfeld aufgezeichneten Kontonummer in die Geschäftstransaktionsdatei **32** geschrieben.

Die Geschäftstransaktionsdatei **32** wird auf die Bank übertragen, für jede Kontonummer umgeordnet und in die Kontodatei **33** geschrieben.

Wenn das Guthaben kleiner wird und der Benutzer erneut einen Bargeldempfang auf die Karte schreiben will, führt er die Karte in das Bankterminal **30** ein und gibt das Kennwort ein. Wenn das Kennwort annehmbar ist, kann die Datei der Karte vom Bankterminal **30** ausgelesen werden. Das Bankterminal liest die Kontonummer von der Karte und öffnet eine Kontodatei, in die bereits Daten vom Geschäft geschrieben worden sind. Eine lautere oder unlautere Behandlung wird daher dadurch unterschieden, daß die Datei der Karte mit der Kontodatei zusammen geführt und der Kontostand geprüft wird.

Wenn beide Aufzeichnungen richtig sind, werden die Aufzeichnungen von der Kartendatei gelöscht.

Wenn alle Aufzeichnungen annehmbar sind, überträgt die Bank die Geldmenge, die der Verbraucher im Geschäft ausgegeben hat. Der Kontostand wird in der Bank berechnet.

Um den Kontostand zu prüfen, werden Barauszahlungen **63** infolge jedes Einkaufs von dem Anfangskontostand der Kartendatei abgezogen, und wird das Ergebnis dieser Subtraktion mit dem Kontostand **64** zusammengezählt.

Wenn die Aufzeichnungen nicht übereinstimmen, wird die Sicherheitscodierung am Terminal für jede der Aufzeichnungen von der Bankdatei auf der Grundlage der Terminalnummer **62** der Aufzeichnungen ausgelesen. Die Sicherheitscodierung und die Aufzeichnung werden dann der Karte eingegeben, um eine Datenänderungsfeststellungscodierung von der Karte zu erhalten. Um diese Codierung mit der Datenänderungsfeststellungscodierung der vorhergehenden Aufzeichnung der Karte oder der Bankdatei zusammen zu führen, wird darauf während der Prüfung der Feststellungscodierung Bezug genommen.

Es sei im folgenden angenommen, daß die Aufzeichnung nicht in Übereinstimmung steht, wobei der Inhalt der Aufzeichnung, der nicht in Übereinstimmung steht, die Zeit ist. In diesem Fall wird die Aufzeichnung der Zeit, die in Übereinstimmung mit irgendeiner der Aufzeichnungen steht, gefunden.

a) Die IC-Karte enthält keine entsprechende Aufzeichnung und die Feststellungscodierungsprüfung der Bankaufzeichnung und die Prüfung des Kontostandes sind in Ordnung. In diesem Fall enthält die Karte keine Aufzeichnung und es wird davon ausgegangen, daß die Aufzeichnung von der IC-Karte gelöscht ist.

b) Die IC-Karte enthält keine entsprechende Aufzeichnung und die Prüfung der Feststellungscodierung der Bankaufzeichnung ist nicht annehmbar. In diesem Fall wurde die Aufzeichnung auf der Seite der Bank zugegeben und es wird davon ausgegangen, daß die Aufzeichnung unberechtigt in die Bankdatei gegeben wurde.

Dieselben Feststellungen können auch dann getroffen werden, wenn auf der Seite der Bank keine entsprechenden Aufzeichnungen vorhanden sind.

Wenn die Aufzeichnung nicht in Übereinstimmung steht, wobei der Inhalt der Aufzeichnung, der nicht in Übereinstimmung steht die Terminalnummer und der Bargeldempfang und die Zahlungen sind, wird eine einwandfreie oder nicht einwandfreie Behandlung dadurch festgestellt, daß jede Feststellungscodierung geprüft wird.

Wenn weiterhin die Aufzeichnung nicht in Übereinstimmung steht und der Inhalt der Kontostand ist wird eine einwandfreie oder nicht einwandfreie Behandlung dadurch festgestellt, daß jeder Kontostand geprüft wird.

Es ist auch erlaubt, statt der Zeitdaten Nummern wie beispielsweise Seriennummern zu verwenden.

Bei dem oben beschriebenen Ausführungsbeispiel der Erfindung ist es möglich, Änderungen der Daten in der IC-Karte oder in der Bankdatei festzustellen.

Im folgenden wird ein drittes Ausführungsbeispiel der erfindungsgemäßen IC-Karte anhand der **Fig. 5** bis 7 beschrieben.

Fig. 5 zeigt in einem Diagramm schematisch den Aufbau eines IC-Kartensystems für Gesundheitsdaten, bei dem die IC-Karte **100** mit einem dafür vorgesehenen Terminal **200** über eine Schnittstelle **290** verbunden ist, um die Funktionen der IC-Karte darzustellen.

Die IC-Karte **100** besteht aus einem Mikroprozessor **120**, einem Festspeicher ROM **110**, einem programmierbaren Festspeicher PROM **130** und einem elektrisch löschbaren programmierbaren Festspeicher EEPROM **140**, die über Signalleitungen **150** miteinander verbunden sind. Wenn die IC-Karte **100** über eine Signalleitung **160** mit dem Terminal **200** für die IC-Karte verbunden ist, wird das Programm im PROM **130** in den Mikroprozessor **120** geladen, so daß es benutzt werden kann.

Das Terminal **200** für die IC-Karte besteht aus einem Mikrocomputer **240**, einer Tastatur **210** und einer Anzeige **220**, die über Signalleitungen **170** miteinander verbunden sind. Der Mikrocomputer **240** ist weiterhin über eine Signalleitung **180**, einen Modem **310**, eine öffentliche Telefonleitung **320** und einen weiteren Modem **330** mit einem Datenverarbeitungszentrum **400** verbunden. Das Datenverarbeitungszentrum **400** besteht aus einem Computer **410** und einer Da-

tenbank **420**.

Der Besitzer der IC-Karte **100** kann einen Arzt aufsuchen, der nicht sein Hausarzt ist, und seine Personenidentifizierungsnummer über die Tastatur **210** eingeben. Das Signal wird dann über den Mikrocomputer **240** auf der Seite des Terminals **200** dem Mikroprozessor **120** in der IC-Karte zugeführt. Der Mikroprozessor **120** führt aber den Speicher ROM **110** einen Suchvorgang durch.

Der ROM **110** hat dabei den in **Fig. 6** dargestellten Datenaufbau. Der Datenaufbau besteht somit aus einer Personenidentifizierungsnummer **111** des Besitzers der IC-Karte **100**, einer Zulässigkeitsstufe **112** des Informationsbezuges des Besitzers, Zulassungscodierungen **113** der praktizierenden zugelassenen Ärzte, deren Personenidentifizierungsnummern **114**, deren Zulässigkeitsstufe **115** des Informationsbezuges, Berechtigungscodierungen **117** der Daten der zugelassenen Ärzte und einer Zulässigkeitsstufe **116** des Informationsbezugs für nicht zugelassene Ärzte.

Wenn der Mikrocomputer **120**, der einen Suchvorgang durch den Speicher ROM **110** ausführt, die Personenidentifizierungsnummer, die eingegeben wird, als übereinstimmend mit der Personenidentifizierungsnummer **111** des Besitzers anzeigt, wird die Zulässigkeitsstufe **112** des Informationsbezuges ausgelesen. Es sei angenommen, daß es nur eine Stufe **1** gibt. Auf der Grundlage dieser Stufe liest der Mikroprozessor **120** die Datei im EEPROM **140**.

Fig. 7 zeigt den Datenaufbau im EEPROM **140**. Dabei sei angenommen, daß die Daten A **141**, die mit der Stufe **1** und der Stufe **2** zugreifbar sind, die Daten B **142**, die nur mit der Stufe **1** zugreifbar sind, im EEROM **140** enthalten sind. Beispielsweise enthalten die Daten A **141** die für die Diagnose und Therapie notwendigen Informationen wie die Blutgruppe, das Diagnoseergebnis einer medizinischen Untersuchung, die Krankengeschichte u. ä. – Die Daten B **142** enthalten Daten wie die familiären Verhältnisse u. a. die keinen direkten Bezug auf die Diagnose und die Therapie haben, sowie diejenigen Daten, von denen der Besitzer der Karte nicht wünscht, daß andere Personen ohne seine Erlaubnis davon Kenntnis erhalten.

In diesem Fall wird die Stufe **1** durch den Mikroprozessor **120** gegeben, um einen Zugriff zu den Daten A **141** und zu den Daten B **142** zu ermöglichen. Die Daten werden nämlich vom Mikroprozessor **120** dem Mikrocomputer **240** für das Terminal zugeführt, einer Verarbeitung zur Anzeige unterworfen und an der Anzeigeeinheit **220** angezeigt. Die Daten werden auch für den Arzt angezeigt, um für die Diagnose und Therapie herangezogen zu werden. Ein Teil der Ergebnisse wird auch über die Tastatur **210** eingegeben und in den Datenbereich A **141** oder den Datenbereich B **142** im EEPROM **140** über den Mikroprozessor **240** den Mikroprozessor **120** u. ä. geschrieben.

Es kann dabei vorkommen, daß der Besitzer der IC-Karte **100** bei einem Verkehrsunfall einer Notbehandlung bedarf, ohne in der Lage zu sein, selbst seine Personenidentifizierungsnummer einzugeben. In diesem Fall gibt der Arzt seine Zulassungscodierung als praktizierender Mediziner und seine Personenidentifizierungsnummer über die Tastatur **210** ein. Das Eingabeergebnis liegt am Mikroprozessor **110** in der IC-Karte **100**, und zwar über den Mikrocomputer **240**. Der Mikroprozessor **120** bildet eine Berechtigungscodierung mit der Personenidentifizierungsnummer **114** als Schlüssel und mit den Daten des zugelassenen Arztes als Eingangsdaten, stellt sicher, ob die in dieser Weise gebildete Zulässigkeitscodierung in Übereinstimmung mit der Zulässigkeitscodierung **117** steht, die in die Datei geschrieben ist, und vergleicht die Zulassungscodierung **113** des niedergelassenen Arztes und die Personenidentifizierungsnummer **114** des zugelassenen Arztes im ROM **110** mit der Zulassungscodierung und der Personenidentifizierungsnummer, die eingegeben sind. Wenn diese Daten übereinstimmen, liest der Mikroprozessor **120** die Zulässigkeitsstufe **115** des Informationsbezuges und die Daten, die dieser Zulässigkeitsstufe genügen, vom EEPROM **140**. Das Ergebnis wird über den Mikroprozessor **120** und den Mikrocomputer **240** an der Anzeigeeinheit **220** angezeigt.

Wenn die Zulassungscodierung des Arztes im entsprechenden ROM **110** gefunden wird, die Personenidentifizierungsnummer jedoch nicht übereinstimmt, wird diese Tatsache an der Anzeigeeinheit **220** angezeigt und wird der Arbeitsvorgang abgeschlossen.

Wenn sogar die Zulassungscodierung des niedergelassenen Arztes im ROM **110** nicht gefunden wird, werden die Zulassungscodierung und die Personenidentifizierungsnummer, die vom Arzt eingegeben werden, dem Datenverarbeitungszentrum **400** zugeführt, wo der Computer **410** zusammenstellt, ob die Datenbank Daten enthält, die mit der Zulassungscodierung und der Personenidentifizierungsnummer übereinstimmen. Wenn das der Fall ist, wird eine geheime Codierung, die die Übereinstimmung anzeigt, der IC-Karte **100** über den Mikrocomputer **240** zugeführt. Die IC-Karte **100** entnimmt die Daten in Abhängigkeit von der Zulässigkeitsstufe **116** des Informationsbezuges für nicht registrierte Ärzte und zeigt die Daten an der Anzeigeeinheit **220** an.

Wenn die Zulassungscodierung des Arztes oder die Personenidentifizierungsnummer des Arztes, die eingegeben wird, nicht übereinstimmt, wird diese Tatsache an der Anzeigeeinheit **220** angezeigt und wird der Arbeitsvorgang abgeschlossen.

Um eine zufällige Übereinstimmung zu vermeiden, die dann auftreten könnte, wenn Daten mehrfach eingegeben werden, ist es erlaubt, die Gegenmaßnahme vorzusehen, daß ein Zugriff nicht mehr möglich ist, wenn eine falsche Personenidentifizierungsnummer mehr als M-mal eingegeben wird, wobei M eine bestimmte Zahl ist. Wenn ein Zugriff zum Datenverarbeitungszentrum erfolgt, kann es weiterhin vorgesehen sein, die Zulassungscodierung des Arztes, die Daten und die Zeit und den Besitzer der Karte in der Datenbank des Datenverarbeitungszentrums zur Datenerfassung zu belassen.

Im vorhergehenden wurden die Fälle beschrieben, bei denen getrennte Inhalte im Speicher ROM **110** und EEPROM **140** gespeichert sind. Die Inhalte können jedoch auch gemeinsam im EEPROM **140** gespeichert sein. Weiterhin kann ein Speicher mit direktem Zugriff RAM statt des EEPROM verwandt werden, vorausgesetzt, daß die Daten gespeichert sind, ohne gelöscht zu werden.

Die vorhergehenden Ausführungsbeispiele befaßten sich mit den Fällen, in denen zwei Zulässigkeitsstufen des Informationsbezuges vorhanden waren. Es versteht sich jedoch, daß auch drei oder mehr Zulässigkeitsstufen des Informationsbezuges vorgesehen sein können.

Obwohl die obige Beschreibung sich weiterhin auf ein IC-Kartensystem für Gesundheitsdaten bezog, eignet sich die erfindungsgemäße Ausbildung auch bei einem IC-Kartensystem für Besitz- oder Vermögensdaten und bei ähnlichen Systemen, bei denen eine dritte qualifizierte Person gezwungen sein kann, auf die Daten in einem Notfall zuzugreifen.

Das erfindungsgemäße System, bei dem ein Bankinstitut die Rolle des IC-Kartenherausgebers spielt und eine IC-Karte für einen Benutzer ausgibt, so daß dieser in einer Vielzahl von Geschäften einkaufen kann, hat die folgenden Vorteile:

1. Schutz der Vertraulichkeit: Daten wie beispiels-

weise der Name des Händlers und der Geldbetrag werden mit Verschlüsselungsbegriffen verschlüsselt, die für die jeweiligen Geschäfte verschieden sind, und auf die IC-Karte geschrieben. Das heißt, daß die Situation, in der die Karte in einem Geschäft benutzt wurde, für die anderen Geschäfte geheim bleibt und die Vertraulichkeit für den Benutzer geschützt wird.

2. Leichte Schlüsselverwaltung: Der IC-Kartenverwalter, der einen Hauptentschlüsselungsbegriff für einen Benutzer hat, kann alle Daten in der IC-Karte entschlüsselt. Der IC-Kartenverwalter benötigt einen geringeren Arbeitsaufwand für die Schlüsselverwaltung beim Begleichen der ausgegebenen Geldbeträge, die in der IC-Karte aufgezeichnet sind.

3. Sicherheit der Schlüsselverwaltung: Der Hauptentschlüsselungsbegriff wird nur vom IC-Kartenverwalter verwaltet und die Zahl der Zugriffe ist relativ klein. Der Hauptentschlüsselungsbegriff kann daher sicher verwaltet werden. Wenn weiterhin ein Geschäft den Verschlüsselungsbegriff oder den Entschlüsselungsbegriff unbeabsichtigt verloren hat, kann der Verschlüsselungsbegriff oder der Entschlüsselungsbegriff in der IC-Karte leicht unter Verwendung des Hauptentschlüsselungsbegriffes der Karte entnommen werde.

4. Es ist möglich, eine Änderung oder Fälschung der Daten in der IC-Karte und in der Bankdatei festzustellen.

5. Im Notfall kann eine dritte qualifizierte Person zu den Daten zugreifen und die Daten zum Nutzen des Besitzers der IC-Karte verwenden.

6. Die Stufe zum Zugriff zu den Daten kann geteilt werden, so daß die Daten innerhalb eines Bereiches einer gegebenen Stufe entnommen werden können. Die Daten, von denen der Besitzer der Karte nicht wünscht, daß andere Personen davon Kenntnis erhalten, können vor dritten Personen geheim gehalten werden.

7. Eine dritte qualifizierte Person klassifiziert die Daten in diejenigen, die in der Karte registriert werden, und diejenigen, die im Verwaltungszentrum registriert werden, so daß dann, wenn ein Arzt diese Daten benutzt, der Arbeitsaufwand und die Kosten für einen Zugriff zum Zentrum über eine Datenverbindungsschaltung herabgesetzt werden können.

Patentansprüche

IC-Karte zum bidirektionalen Datentransfer mit einer Vielzahl von Terminals (**9** bis **11**), auf der ein Berechtigungscode für die Benutzung der Vielzahl von Terminals durch einen Benutzer (**16**) der IC-Karte gespeichert und auf der ein Speicher (**19**) vorgesehen ist, der in eine Vielzahl von Bereichen (**22** bis **24**) aufgeteilt ist, **dadurch gekennzeichnet**, daß

jedem der Bereiche ein eigenes Verschlüsselungs- und Entschlüsselungsbegriffspaar (**102** bis **107**) zugeordnet ist,

wobei die verschiedenen Verschlüsselungs- und Entschlüsselungsbegriffspaare jeweils einer Anzahl von Personen, die die Terminals (**9** bis **11**) betreiben, bekanntgegeben werden, um die IC-Karte für diese Anzahl von Personen verwendbar zu gestalten,

wobei die Daten jedes Bereiches bei Eingabe des dem Bereich zugeordneten Verschlüsselungsbegriffes an einem der Terminals verschlüsselt werden, und

wobei die Daten jedes Bereiches bei Eingabe des dem Bereich zugeordneten Entschlüsselungsbegriffes an einem der Terminals entschlüsselt werden.

Hierzu 5 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 37 04 814 C3
Int. Cl.[7]: G 06 K 19/073
Veröffentlichungstag: 2. Mai 1996

FIG. 1A

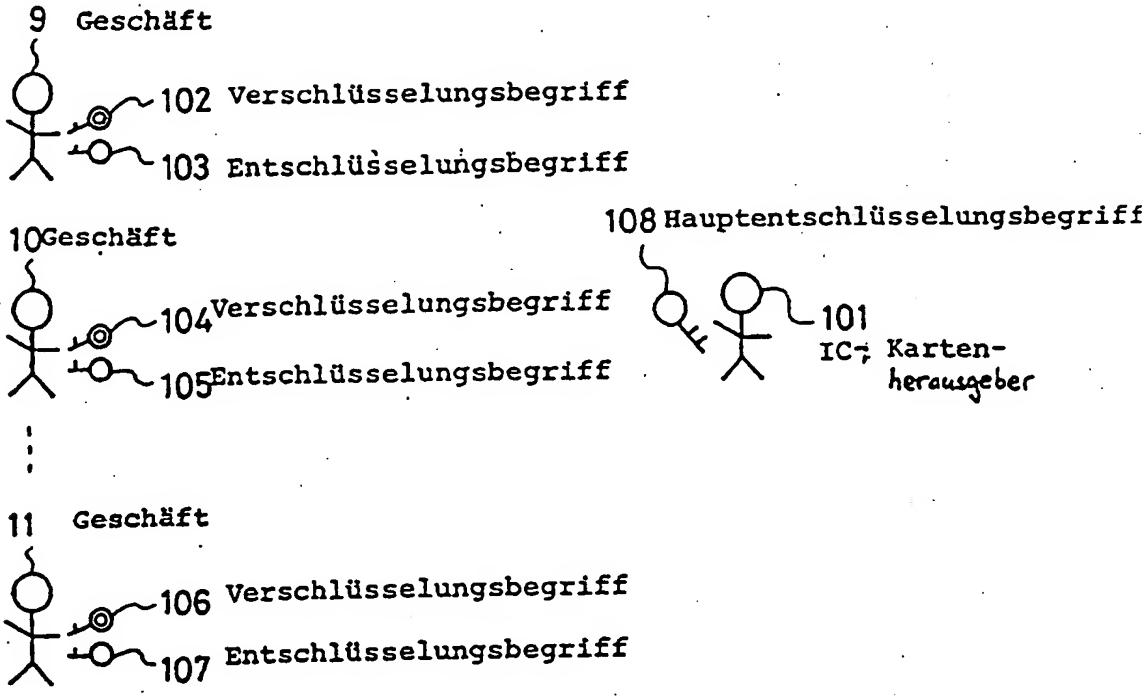
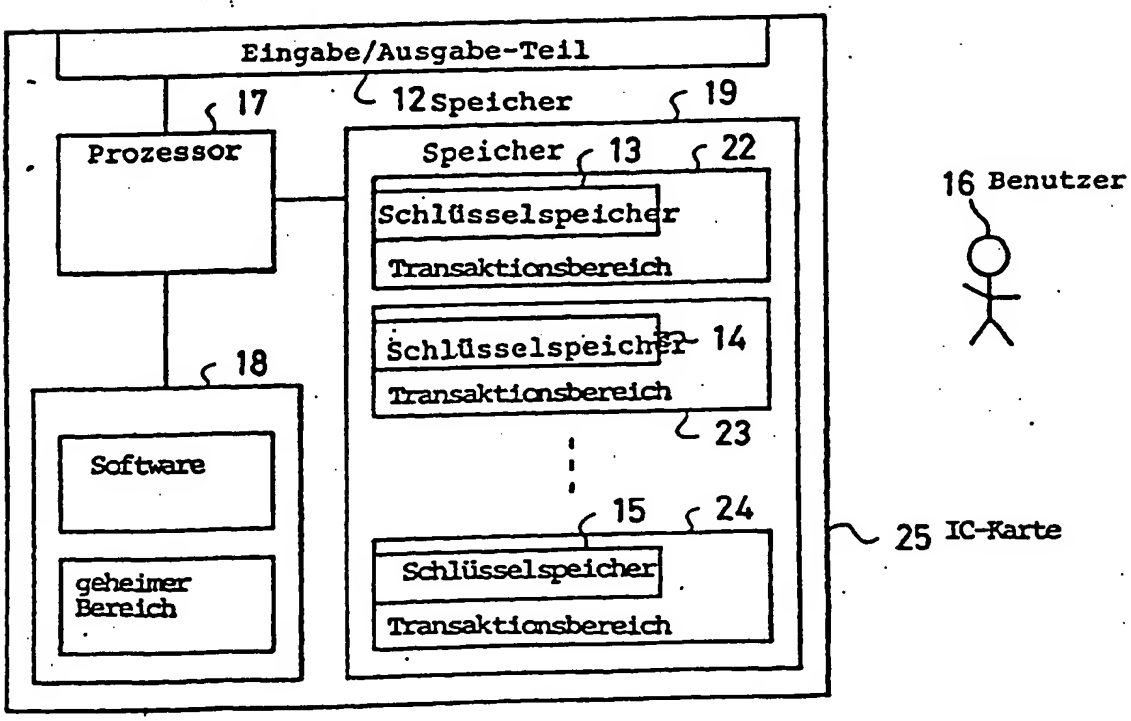
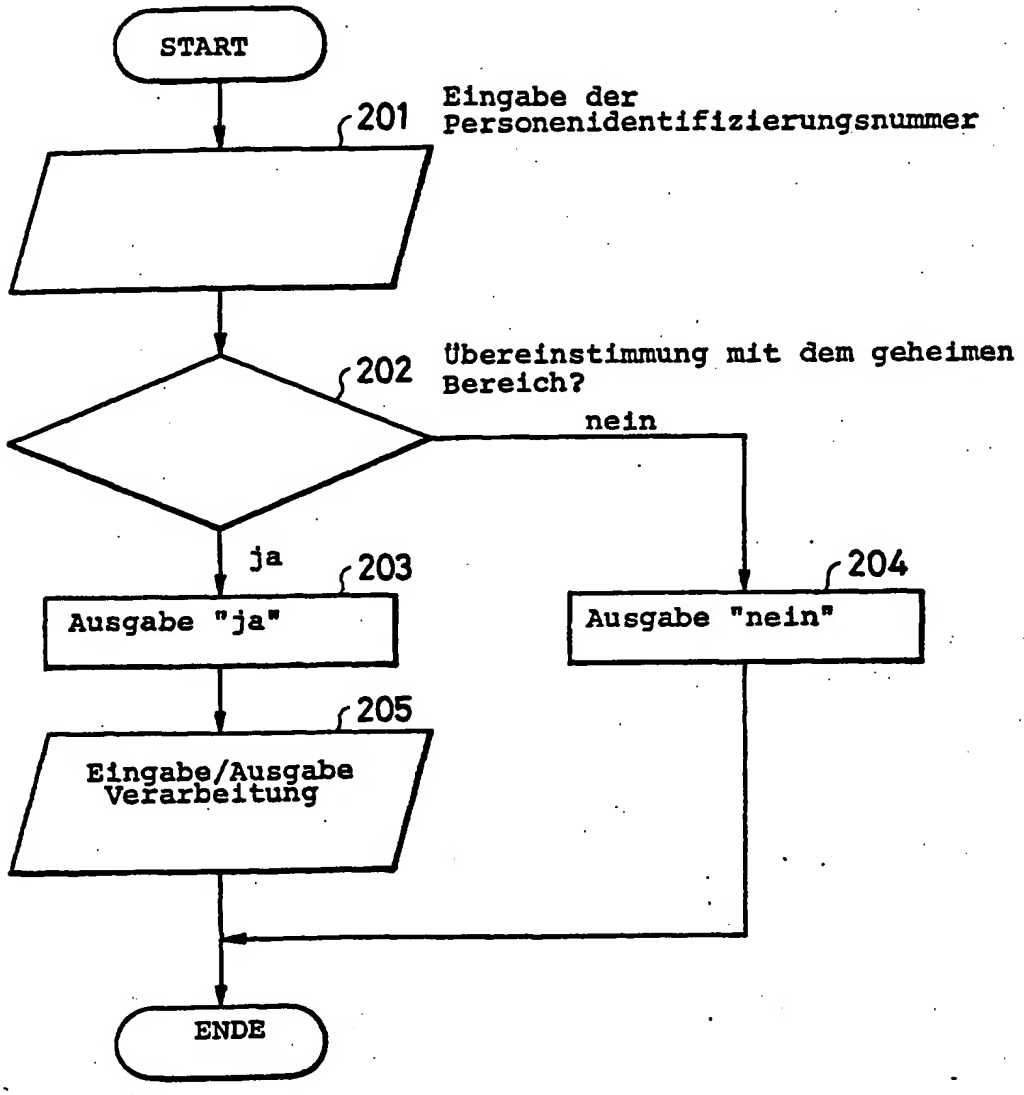


FIG. 1B



Nummer: DE 37 04 814 C3
Int. Cl.[7]: G 06 K 19/073
Veröffentlichungstag: 2. Mai 1996

FIG. 2



Nummer: DE 37 04 814 C3
Int. Cl.[7]: G 06 K 19/073
Veröffentlichungstag: 2. Mai 1996

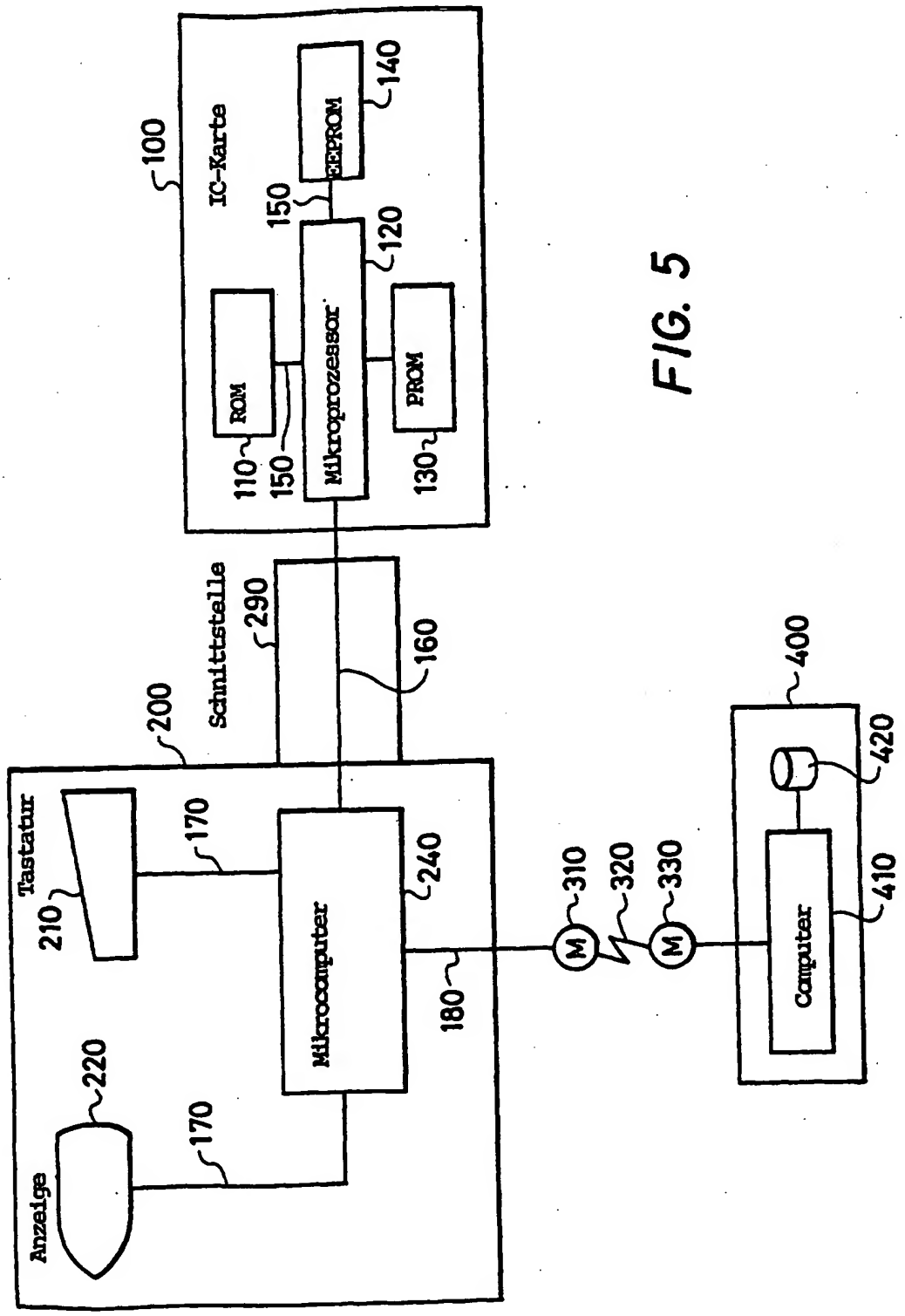


FIG. 5

Nummer: DE 37 04 814 C3
Int. Cl.[7]: G 06 K 19/073
Veröffentlichungstag: 2. Mai 1996

FIG. 6

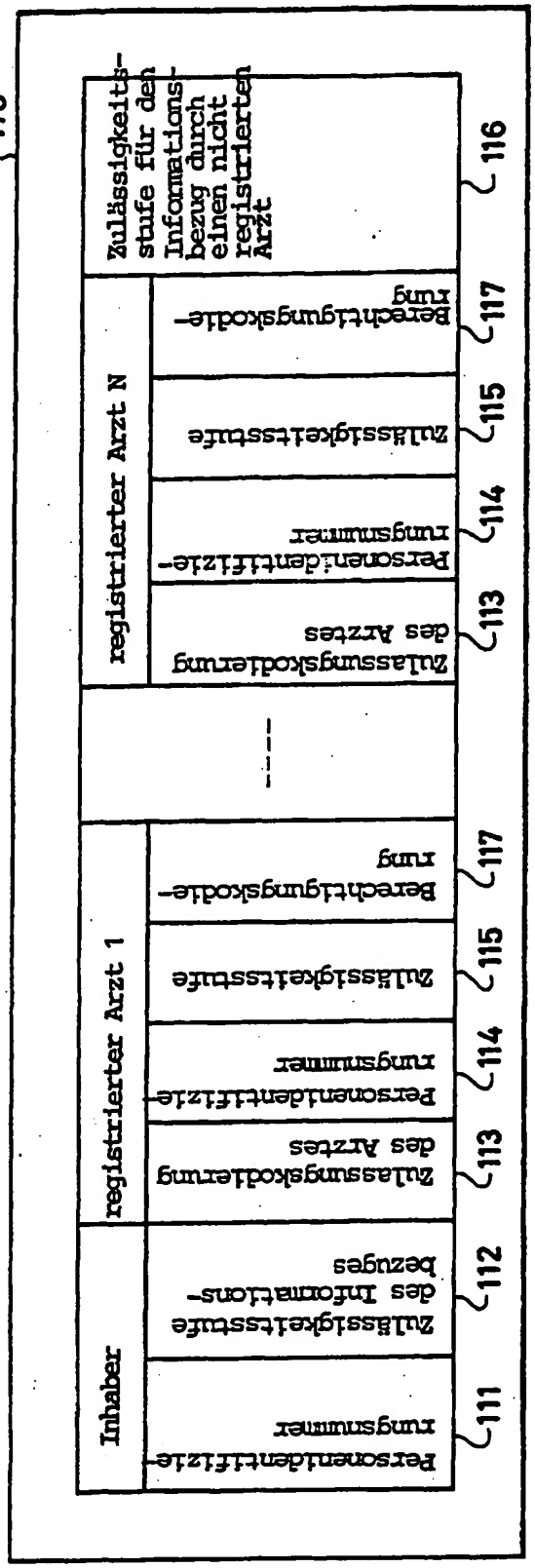


FIG. 7